Migrar de EzVPN-NEM+ heredada a FlexVPN en el mismo servidor

Contenido

Introducción

Este documento describe el proceso de migración de EzVPN a FlexVPN. FlexVPN es la nueva solución de VPN unificada que ofrece Cisco. FlexVPN se beneficia del protocolo IKEv2 y combina el acceso remoto, de sitio a sitio, de hub y spoke, así como implementaciones de VPN de malla parcial. Con tecnologías heredadas como EzVPN, Cisco le anima a migrar a FlexVPN para aprovechar sus capacidades repletas de funciones.

Este documento examina una implementación EzVPN existente que consta de clientes de hardware EzVPN heredados que terminan los túneles en un dispositivo de cabecera EzVPN basado en crypto map heredado. El objetivo es migrar desde esta configuración para admitir FlexVPN con estos requisitos:

- Los clientes antiguos existentes seguirán trabajando sin problemas sin que se produzcan cambios en la configuración. Esto permite una migración por fases de estos clientes a

FlexVPN con el tiempo.
- El dispositivo de cabecera debe admitir simultáneamente la terminación de nuevos clientes FlexVPN.

Se utilizan dos componentes de configuración IPsec clave para ayudar a alcanzar estos objetivos de migración: a saber, IKEv2 e Interfaces de túnel virtual (VTI). Estos objetivos se examinan brevemente en este documento.

Otros documentos de esta serie

- Guía de implementación de FlexVPN: AnyConnect con IOS Headend Over IPsec con IKEv2 y certificados

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

IKEv1 frente a IKEv2

FlexVPN se basa en el protocolo IKEv2, que es el protocolo de administración de claves de última generación basado en RFC 4306, y una mejora del protocolo IKEv1. FlexVPN no es compatible con versiones anteriores con tecnologías que solo admiten IKEv1 (por ejemplo, EzVPN). Esta es una de las consideraciones clave al migrar de EzVPN a FlexVPN. Para ver una introducción del protocolo en IKEv2 y la comparación con IKEv1, consulte IKE versión 2 de un vistazo.

Mapa criptográfico frente a interfaces de túnel virtual

La interfaz de túnel virtual (VTI) es un nuevo método de configuración utilizado tanto para las configuraciones de servidor VPN como de cliente. VTI:

- Sustitución de mapas criptográficos dinámicos, que ahora se considera configuración heredada.
- Admite tunelización IPsec nativa.
- No requiere un mapping estático de una sesión IPSec a una interfaz física; por lo tanto, proporciona flexibilidad para enviar y recibir tráfico cifrado en cualquier interfaz física (por ejemplo, varias rutas).

- La configuración mínima como acceso virtual a demanda se clona desde la interfaz de plantilla virtual.
- El tráfico se cifra/descifra cuando se reenvía a/desde la interfaz de túnel y se administra mediante la tabla de IP Routing (por lo tanto, desempeña un papel importante en el proceso de cifrado).
- Las funciones se pueden aplicar a los paquetes de texto sin cifrar en la interfaz VTI o a los paquetes cifrados en la interfaz física.

Los dos tipos de VTI disponibles son:

- Estático (sVTI): una interfaz de túnel virtual estática tiene un origen y un destino de túnel fijos y se suele utilizar en un escenario de implementación de sitio a sitio. Este es un ejemplo de una configuración de sVTI:

```
interface Tunnel2
 ip address negotiated
 tunnel source Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile testflex
```

- Dinámico (dVTI): se puede utilizar una interfaz de túnel virtual dinámica para finalizar túneles IPsec dinámicos que no tienen un destino de túnel fijo. Tras una negociación de túnel exitosa, las interfaces de acceso virtual se clonarán a partir de una plantilla virtual y heredarán todas las funciones de L3 de esa plantilla virtual. Este es un ejemplo de una configuración dVTI:

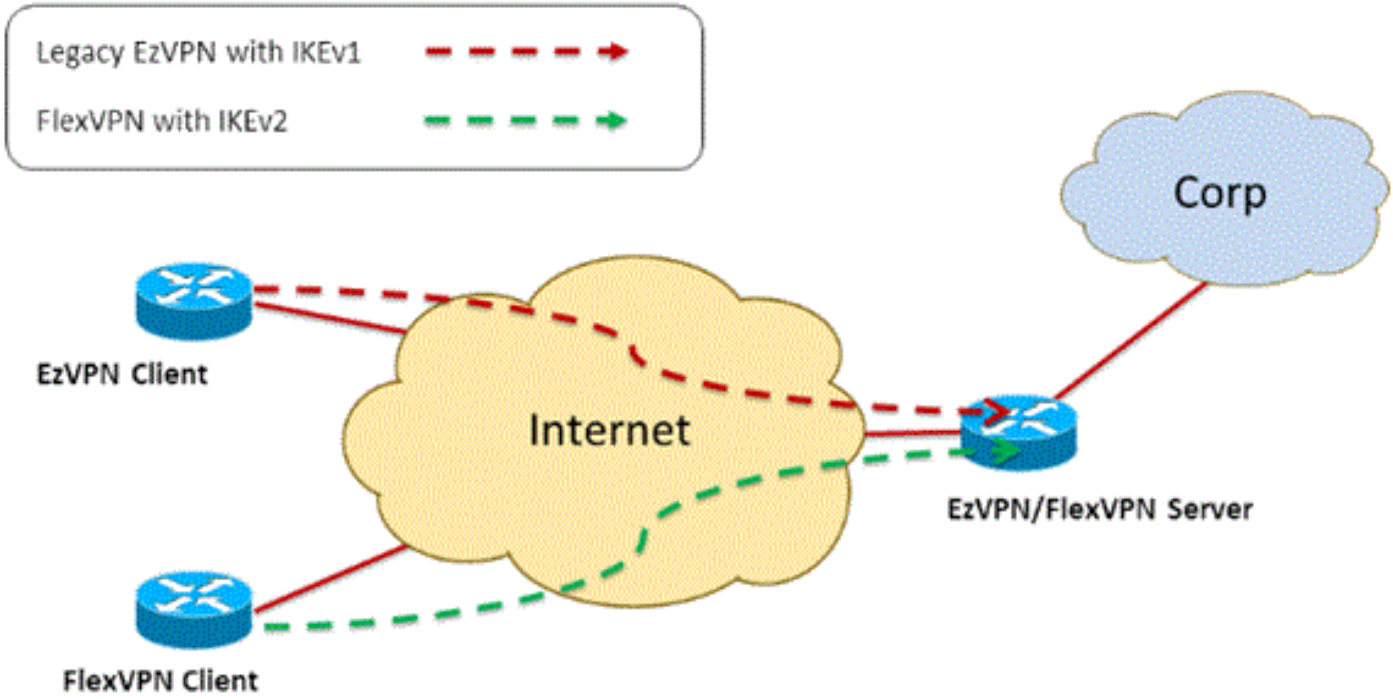
```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile testflex
```

Consulte estos documentos para obtener más información sobre dVTI:

- Configuración de Cisco Easy VPN con interfaz de túnel virtual dinámica (DVTI) IPSec
- Restricciones de IPsec Virtual Tunnel Interface
- Configuración del Soporte Multi-SA para Interfaces de Túnel Virtual Dinámicas Usando IKEv1

Para que los clientes EzVPN y FlexVPN coexistan, primero debe migrar el servidor EzVPN de la configuración de mapa crypto heredada a una configuración dVTI. En las secciones siguientes se explican en detalle los pasos necesarios.

Topología de red



Configuración actual con cliente EzVPN de modo NEM+ heredado

Configuración del Cliente

A continuación se muestra una configuración típica del router cliente EzVPN. En esta configuración, se utiliza el modo Network Extension Plus (NEM+), que crea varios pares SA tanto para las interfaces internas LAN como para la configuración de modo asignada a la dirección IP para el cliente.

```
crypto ipsec client ezvpn legacy-client
 connect manual
 group Group-One key cisco123
 mode network-plus
 peer 192.168.1.10
 username client1 password client1
 xauth userid mode local
!
interface Ethernet0/0
 description EzVPN WAN interface
 ip address 192.168.2.101 255.255.255.0
 crypto ipsec client ezvpn legacy-client
!
interface Ethernet1/0
 description EzVPN LAN inside interface
 ip address 172.16.1.1 255.255.255.0
 crypto ipsec client ezvpn legacy-client inside
```

Configuración del servidor

En el servidor EzVPN, se utiliza una configuración de mapa crypto heredada como configuración base antes de la migración.

```
aaa new-model
!
aaa authentication login client-xauth local
aaa authorization network ezvpn-author local
!
username client1 password 0 client1
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp client configuration group Group-One
 key cisco123
 pool Group-One-Pool
 acl split-tunnel-acl
crypto isakmp profile Group-One-Profile
   match identity group Group-One
   client authentication list client-xauth
   isakmp authorization list ezvpn-author
   client configuration address respond
!
crypto ipsec transform-set aes-sha esp-aes esp-sha-hmac
!
crypto dynamic-map client-dynamic-map 1
 set transform-set aes-sha
 reverse-route
!
crypto map client-map 1 ipsec-isakmp dynamic client-dynamic-map
!
interface Ethernet0/0
 description EzVPN server WAN interface
 ip address 192.168.1.10 255.255.255.0
 crypto map client-map
!
ip local pool Group-One-Pool 10.1.1.100 10.1.1.200
!
ip access-list extended split-tunnel-acl
  remark EzVPN split tunnel ACL
 permit ip 172.16.0.0 0.0.0.255 any
```

Migración del servidor a FlexVPN

Como se describe en las secciones anteriores, FlexVPN utiliza IKEv2 como protocolo del plano de control y no es compatible con una solución EzVPN basada en IKEv1. Como resultado, la idea general de esta migración es configurar el servidor EzVPN existente de forma que permita que tanto EzVPN (IKEv1) como FlexVPN (IKEv2) antiguos coexistan. Para lograr este objetivo, puede utilizar este enfoque de migración de dos pasos:

1. Mueva la configuración EzVPN heredada en la cabecera de una configuración basada en mapa crypto a dVTI.
2. Agregue la configuración de FlexVPN, que también se basa en dVTI.

Mover mapa criptográfico heredado a dVTI

Cambios en la configuración del servidor

Un servidor EzVPN configurado con crypto map en la interfaz física incluye varias limitaciones cuando se trata de compatibilidad y flexibilidad de funciones. Si tiene EzVPN, Cisco le recomienda encarecidamente que utilice dVTI en su lugar. Como primer paso para migrar a una configuración EzVPN y FlexVPN coexistente, debe cambiarla a una configuración dVTI. Esto proporcionará separación IKEv1 e IKEv2 entre las diferentes interfaces de plantilla virtual para acomodar ambos tipos de clientes.

Nota: Para soportar el modo Network Extension Plus de la operación EzVPN en los clientes EzVPN, el router de cabecera debe tener soporte para la función multi SA en dVTI. Esto permite que el túnel proteja varios flujos IP, lo que es necesario para que el centro distribuidor cifre el tráfico a la red interna del cliente EzVPN, así como la dirección IP asignada al cliente a través de la configuración de modo IKEv1. Para obtener más información sobre el soporte de SA múltiple en dVTI con IKEv1, refiérase a Soporte Multi-SA para Interfaces de Túnel Virtual Dinámicas para IKEv1.

Complete estos pasos para implementar el cambio de configuración en el servidor:

Paso 1: elimine el mapa criptográfico de la interfaz de salida física que termina los túneles de cliente EzVPN:

```
interface Ethernet0/0
 ip address 192.168.1.10 255.255.255.0
 no crypto map client-map
```

Paso 2: cree una interfaz de plantilla virtual desde la que se clonarán las interfaces de acceso virtual una vez que se hayan establecido los túneles:

```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet1/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile legacy-profile
```

Paso 3: asocie esta interfaz de plantilla virtual creada recientemente al perfil isakmp para el grupo EzVPN configurado:

```
crypto isakmp profile Group-One-Profile
   match identity group Group-One
   client authentication list client-xauth
   isakmp authorization list ezvpn-author
   client configuration address initiate
   client configuration address respond
   virtual-template 1
```

Una vez realizados los cambios de configuración anteriores, verifique que los clientes EzVPN existentes sigan funcionando. Sin embargo, ahora sus túneles se terminan en una interfaz de acceso virtual creada dinámicamente. Esto se puede verificar con el comando **show crypto session** como en este ejemplo:

```
PE-EzVPN-Server#show crypto session
Crypto session current status
Interface: Virtual-Access1
Username: client1
Profile: Group-One-Profile
Group: Group-One
```

```
Assigned address: 10.1.1.101
Session status: UP-ACTIVE
Peer: 192.168.2.101 port 500
  IKEv1 SA: local 192.168.1.10/500 remote 192.168.2.101/500 Active
  IPSEC FLOW: permit ip 172.16.0.0/255.255.255.0 host 10.1.1.101
        Active SAs: 2, origin: crypto map
  IPSEC FLOW: permit ip 172.16.0.0/255.255.255.0 172.16.1.0/255.255.255.0
        Active SAs: 2, origin: crypto map
```

Agregar la configuración FlexVPN al servidor

Este ejemplo utiliza RSA-SIG (es decir, Autoridad de Certificación) tanto en el cliente FlexVPN como en el servidor. La configuración de esta sección supone que el servidor ya se ha autenticado e inscrito correctamente con el servidor CA.

Paso 1: verifique la configuración IKEv2 Smart Default.

Con IKEv2, ahora puede aprovechar la función Smart Default introducida en 15.2(1)T. Se utiliza para simplificar la configuración de FlexVPN. Estas son algunas configuraciones predeterminadas:

Política de autorización IKEv2 predeterminada:

```
VPN-Server#show crypto ikev2 authorization policy default
 IKEv2 Authorization Policy : default
 route set interface
 route accept any tag : 1 distance : 1
```

Propuesta IKEv2 predeterminada:

```
VPN-Server#show crypto ikev2 proposal default
 IKEv2 proposal: default
 Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
 Integrity : SHA512 SHA384 SHA256 SHA96 MD596
 PRF : SHA512 SHA384 SHA256 SHA1 MD5
 DH Group : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

Política IKEv2 predeterminada:

```
VPN-Server#show crypto ikev2 policy default
 IKEv2 policy : default
 Match fvrf : any
 Match address local : any
 Proposal : default
```

Perfil IPsec predeterminado:

```
VPN-Server#show crypto ipsec profile default
IPSEC profile default
 Security association lifetime: 4608000 kilobytes/3600 seconds
 Responder-Only (Y/N): N
 PFS (Y/N): N
 Transform sets={
 default: { esp-aes esp-sha-hmac } ,
 }
```

Conjunto de transformación IPSec predeterminado:

```
VPN-Server#show crypto ipsec transform default
{ esp-aes esp-sha-hmac }
 will negotiate = { Transport, },
```

Para obtener más información sobre la función IKEv2 Smart Default, refiérase a IKEv2 Smart Defaults (sólo clientes registrados) .

Paso 2: modifique la política de autorización IKEv2 predeterminada y agregue un perfil IKEv2 predeterminado para los clientes FlexVPN.

El perfil IKEv2 creado aquí coincidirá con un ID de peer basado en el nombre de dominio cisco.com y las interfaces de acceso virtual creadas para los clientes se generarán a partir de la plantilla virtual 2. Tenga en cuenta también que la política de autorización define el conjunto de direcciones IP utilizado para asignar direcciones IP de peer así como las rutas que se intercambiarán a través del modo de configuración IKEv2:

```
crypto ikev2 authorization policy default
 pool flexvpn-pool
 def-domain cisco.com
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn VPN-Server.cisco.com
 authentication remote pre-share
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
 virtual-template 2
```

Paso 3: cree la interfaz de plantilla virtual utilizada para los clientes FlexVPN:

```
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet1/0
 tunnel protection ipsec profile default
```

Configuración de cliente FlexVPN

```
crypto ikev2 authorization policy default
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Client2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
```

```
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.10
 tunnel protection ipsec profile default
```

Configuración completada

Configuración de servidor híbrido completa

```
hostname VPN-Server
!
!
aaa new-model
!
aaa authentication login client-xauth local
aaa authorization network default local
aaa authorization network ezvpn-author local
!
!
no ip domain lookup
ip domain name cisco.com
ip host ca-server 192.168.2.1
!
crypto pki trustpoint flex-trustpoint
 enrollment url http://ca-server:80
 serial-number
 ip-address none
 fingerprint 08CBB1E948A6D9571965B5EE58FBB726
 subject-name cn=vpn-server.cisco.com, OU=Flex, O=cisco
 revocation-check crl
 rsakeypair flex-key-pair 1024
!
!
crypto pki certificate chain flex-trustpoint
 certificate 07
 certificate ca 01
username client1 password 0 client1
username cisco password 0 cisco
!
crypto ikev2 authorization policy default
 pool flexvpn-pool
 def-domain cisco.com
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn VPN-Server.cisco.com
 authentication remote pre-share
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
 virtual-template 2
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
```

```
crypto isakmp client configuration group Group-One
 key cisco123
 pool Group-One-Pool
 acl split-tunnel-acl
 save-password
crypto isakmp profile Group-One-Profile
 match identity group Group-One
 client authentication list client-xauth
 isakmp authorization list ezvpn-author
 client configuration address initiate
 client configuration address respond
 virtual-template 1
!
crypto ipsec transform-set aes-sha esp-aes esp-sha-hmac
!
crypto ipsec profile default
 set ikev2-profile default
!
crypto ipsec profile legacy-profile
 set transform-set aes-sha
!
crypto dynamic-map client-dynamic-map 1
 set transform-set aes-sha
 reverse-route
!
crypto map client-map 1 ipsec-isakmp dynamic client-dynamic-map
!
interface Ethernet0/0
 description WAN
 ip address 192.168.1.10 255.255.255.0
!
interface Ethernet1/0
 description LAN
 ip address 172.16.0.1 255.255.255.0
!
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet1/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile legacy-profile
!
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet1/0
 tunnel protection ipsec profile default
!
ip local pool Group-One-Pool 10.1.1.100 10.1.1.200
ip local pool flexvpn-pool 10.1.1.201 10.1.1.250
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
ip access-list extended split-tunnel-acl
 remark EzVPN split tunnel ACL
 permit ip 172.16.0.0 0.0.0.255 any
!
access-list 1 permit 172.16.0.0 0.0.0.255
```

Configuración completa del cliente IKEv1 EzVPN

```
hostname Client1
!
crypto ipsec client ezvpn legacy-client
```

```
 connect manual
 group Group-One key cisco123
 mode network-extension
 peer 192.168.1.10
 username client1 password client1
 xauth userid mode local
!
interface Ethernet0/0
 description WAN
 ip address 192.168.2.101 255.255.255.0
 crypto ipsec client ezvpn legacy-client
!
interface Ethernet1/0
 description LAN
 ip address 172.16.1.1 255.255.255.0
 crypto ipsec client ezvpn legacy-client inside
!
ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

Configuración completa de IKEv2 FlexVPN Client

```
hostname Client2
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization network default local
!
!
no ip domain lookup
ip domain name cisco.com
ip host ca-server 192.168.2.1
!
crypto pki trustpoint flex-trustpoint
 redundancy
 enrollment url http://ca-server:80
 serial-number
 ip-address none
 fingerprint 08CBB1E948A6D9571965B5EE58FBB726
 subject-name cn=Client2.cisco.com, OU=Flex, O=cisco
 revocation-check crl
 rsakeypair flex-key-pair 1024
!
!
crypto pki certificate chain flex-trustpoint
 certificate 06
 certificate ca 01
!
!
crypto ikev2 authorization policy default
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Client2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
```

```
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.10
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 description WAN
 ip address 192.168.2.102 255.255.255.0
!
interface Ethernet1/0
 description LAN
 ip address 172.16.2.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.2.1
!
access-list 1 permit 172.16.2.0 0.0.0.255
```

Verificación de la configuración

Estos son algunos de los comandos usados para verificar las operaciones EzVPN/FlexVPN en un router:

```
show crypto session

show crypto session detail

show crypto isakmp sa

show crypto ikev2 sa

show crypto ipsec sa detail

show crypto ipsec client ez (for legacy clients)

show crypto socket

show crypto map
```

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems